MINISTRY OF EDUCATION
TE TĀHUHU O TE MĀTAURANGA

Privacy Impact Assessment

Targeted Funding for Disadvantage in Early Childhood Education (ECE)

Last Published Date: 11 August 2017

1 Introduction and overview

1.1 Introduction

1.1.1 The Ministry Privacy and Information Security Strategy aims to raise the Ministry's privacy and information security capability through:

- Creating the appropriate Privacy and Information Security Frameworks (e.g. Policies and Standards, Risk Assessment Tools).
- Establishing specific Privacy and Information Security Programmes and targeted business-focused controls, including:
    - Privacy and Security by Design.
    - Risk Assessment.
    - System Certification and Accreditation.

1.1.2 The Privacy Impact Assessment (PIA) process is an input to the System Certification and Accreditation process. The Ministry follows the guidance of the Office of the Privacy Commissioner for undertaking a PIA. Refer to the Privacy Impact Assessment Toolkit[1] for more information.

1.1.3 A PIA is used to assess the privacy impacts of proposed changes that affect personal information, whether the information is about clients, employers, providers or staff. A full PIA will only be necessary for projects that will significantly impact on client and customer privacy.

1.1.4 This PIA considers a new ECE initiative, TFD. TFD will provide additional funding to services and ngā kōhanga reo with relatively high proportions of FCH attended by children at greater risk of educational underachievement due to disadvantage.

1.1.5 TFD will be transitioned into a new system in 2020 that will operate within the IDI (Integrated Data Infrastructure). At that point the risks contained within this PIA will no longer be relevant.

1.2 Purpose, scope and assumptions

PURPOSE

1.2.1 The purpose of this PIA is to:

- Identify the potential effects that TFD may have upon the personal privacy of users and individuals about whom personal information is held by the Ministry for TFD.
- Identify how any detrimental effects on, or risks to, privacy can be lessened and/or managed.
- Recommend controls and responses to enhance the privacy of personal information collected and stored by the Ministry for TFD.

SCOPE

1.2.2 The scope of this report is a PIA for TFD specifically including the following activities:

- An analysis of the full life cycle of personal data including the collection, usage, retention and destruction of personal data. This is particularly relevant for the MSD data, which the Ministry will have no use for after the data match. There will also be clear descriptions of the different stages of the process and how personal information will be used at each of them. This will include diagrams such as the one annexed on page 15, that show how data are managed and used, eg within the Education Management Information System (EDUMIS).

[1] https://www.privacy.org.nz/news-and-publications/guidance-resources/privacy-impact-assessment/

- A description of the information used and how it will be used. This will include the legal grounds of use and clarification of what the information can and cannot be used for. The information will be Early Learning Information (ELI) data on per-child attendance, MSD data on benefit receipt, Te Kōhanga Reo (TKR) data on per-child attendance, and 2015 ECE Census data used in the regression.
- An identification and assessment of the privacy risks. These will be assessed using the Ministry's risk framework. This includes a risk matrix, which classifies risks according to the likelihood of them occurring and the severity of the impact if they did. These risks will be linked to the affected IPPs. These twelve principles come from the Privacy Act 1993 and deal with issues such as the collection and retention of personal information.
- Description of the controls to reduce the residual risk of any identified privacy risks. Generally, these controls include privacy enhancing responses, such as confidentiality thresholds, and security controls, such as role based access control.
- Description of any recommended practices and processes to assure continued compliance to the privacy principles. This will include the controls already mentioned but also the circumstances in which the PIA might have to be revised and who should be responsible for ensuring the privacy controls are maintained.
- The information that we will give to services who receive funding – ie their percentage of Targeted Hours.

1.2.3 Specifically *excluded* from the scope of this PIA are:

- The current ELI process of data collection and storage. This has already been assessed under a separate PIA, which is currently being revised.
- The transition to per-child ECE funding in 2020. This should be covered in a separate PIA to avoid making it more difficult to identify the relevant principles and concerns.

ASSUMPTIONS

1.2.4 The following assumptions are in place for this PIA:

- The ELI PIA completed in 2014 and the current revision of that PIA has captured all the relevant privacy risks of the ELI system, other than using ELI data for funding purposes.
- The collection of personal information by MSD and TKR has been done in accordance with the Privacy Act, prior to that information being received by the Ministry, and therefore will not be challenged under this PIA.
- That RS7 data used in the funding calculation does not contain personal information, as it does not identify any children and only aggregates information at a service level by asking for the number of FCH. Therefore, this PIA will not look at RS7 data.

1.3 Glossary of Terms

This table lists and defines terms used in this document.

Term	Definition
ECE	Early Childhood Education
EDUMIS	Education Management Information System
ELI	Early Learning Information
EQI	Equity Index
FCH	Funded Child Hours

Term	Definition
IDI	Integrated Data Infrastructure
IPP	Information Privacy Principle
MoE	Ministry of Education
MOU	Memorandum of Understanding
MSD	Ministry of Social Development
NSN	National Student Number
PIA	Privacy Impact Assessment
SMS	Student Management System
SWN	Social Welfare Number
TFD	Targeted Funding for Disadvantage
TKR	Te Kōhanga Reo

2 Description of the project and information flows

2.1 Proposal

2.1.1 TFD is a new initiative that will target additional funding to ECE services and ngā kōhanga reo with relatively high proportions of FCH attended by children at greater risk of educational underachievement due to disadvantage.

2.1.2 Each child attending ECE will be given a risk score based on the proportion of their life they have been the dependent of a beneficiary. The 20% of children with the highest risk scores will be considered at greater risk of educational underachievement due to disadvantage.

2.1.3 Our research shows that children who have been the dependent of a beneficiary for a significant period of their life are at greater risk of educational underachievement.

2.1.4 Per-child attendance data will be used to estimate the percentage of FCH attended by children at risk of underachievement in each service. This will be done through a data match between per-child attendance data, (including from the ELI system from the period 1 July 2016 – 30 June 2016) and the MSD benefit receipt records.

2.1.5 This will be the first time that ELI data has been used to calculate funding. The ELI PIA from 2014 recommends that if ELI data is used for funding purposes then another PIA should be completed.

2.1.6 A similar PIA was recently completed as part of the Funding Review around the use of a predictive risk index. This covered the use of data from the Integrated Data Infrastructure (IDI), managed by Statistics NZ. It did not cover TFD, which will require the matching of data within the Ministry. This is different to receiving anonymised data from the IDI and raises different privacy risks.

2.2 Business context

2.2.1 As more government services are provided digitally, it is imperative that New Zealand citizens have and maintain trust and confidence in government as a responsible steward of personal information. The Ministry, as the collector and custodian of information about children in ECE, wishes to ensure that all reasonable steps are taken to preserve the privacy of this information and that the trust and confidence of the sector and the New Zealand public is maintained.

2.2.2 Although services will not be told which children are at risk of educational underachievement due to disadvantage and the additional funding is not targeted to individuals, there are privacy risks to individuals and consequent risks to the Ministry that arise through combining information in this way. For example, an information breach could occur that meant a group of children were identified as at risk of underachievement. This could result in stigmatisation of the children and their families. This would also reflect badly on the Ministry and damage their credibility.

2.3 Legal context

2.3.1 The Ministry and TFD must comply with the Privacy Act 1993 which protects information about individuals. It applies to every agency (public and private) that deals with personal information. Twelve IPPs in the Act provide a foundation that governs the protection of privacy in regard to the collection, use, disclosure, storage and access to personal information.

2.3.2 The Ministry must also operate in accordance with the Education Act 1989, the Public Records Act 2005, and the Official Information Act 1982.

2.3.3 The Ministry's internal legal services have confirmed that the proposal to use ELI information for funding purposes is consistent with both the Privacy Act 1993 and the Education Act 1989. They also noted that data matching issues under the Privacy Act 1993 will not arise as there are no adverse consequences as a result of the matching of MSD information with MOE information.

2.4 Information Flows

IDENTITY ATTRIBUTES

2.4.1 TFD uses a range of different personal information, which is detailed in the table below.

Source of personal information	Type of personal information
MSD	• Child's given name • Child's last name • Child's gender • Child's date of birth • Parent's ID – Social Welfare Number (SWN) • Benefit type • Benefit group • Period spent on benefit • If it is a current record
ELI	• Child's first name • Child's middle name • Child's last name • Child's gender • Child's date of birth • Attendance data • Attendance hours • Absent hours • Service ID • Service name
TKR	• Child's ID • Child's first name • Child's middle name • Child's last name • Child's gender • Child's date of birth • Child's ethnicity • Attendance dates • Attendance hours • Absent hours

Source of personal information	Type of personal information
	• Kōhanga ID • Kōhanga name
ECE Census	• While technically the ECE Census does not contain any personal information, as it is all aggregated at a service level, in some cases the reporting of children by gender, ethnicity and age could lead to particular children being identified. Therefore it is included in this PIA. • Total number of male children attending/enrolled at the service • Total number of Maori children attending/enrolled at the service • Total number of Pasifika children attending/enrolled at the service • Total number of other children attending/enrolled at the service • Total number of children attending/enrolled at the service • Equity Index (EQI) score of the service

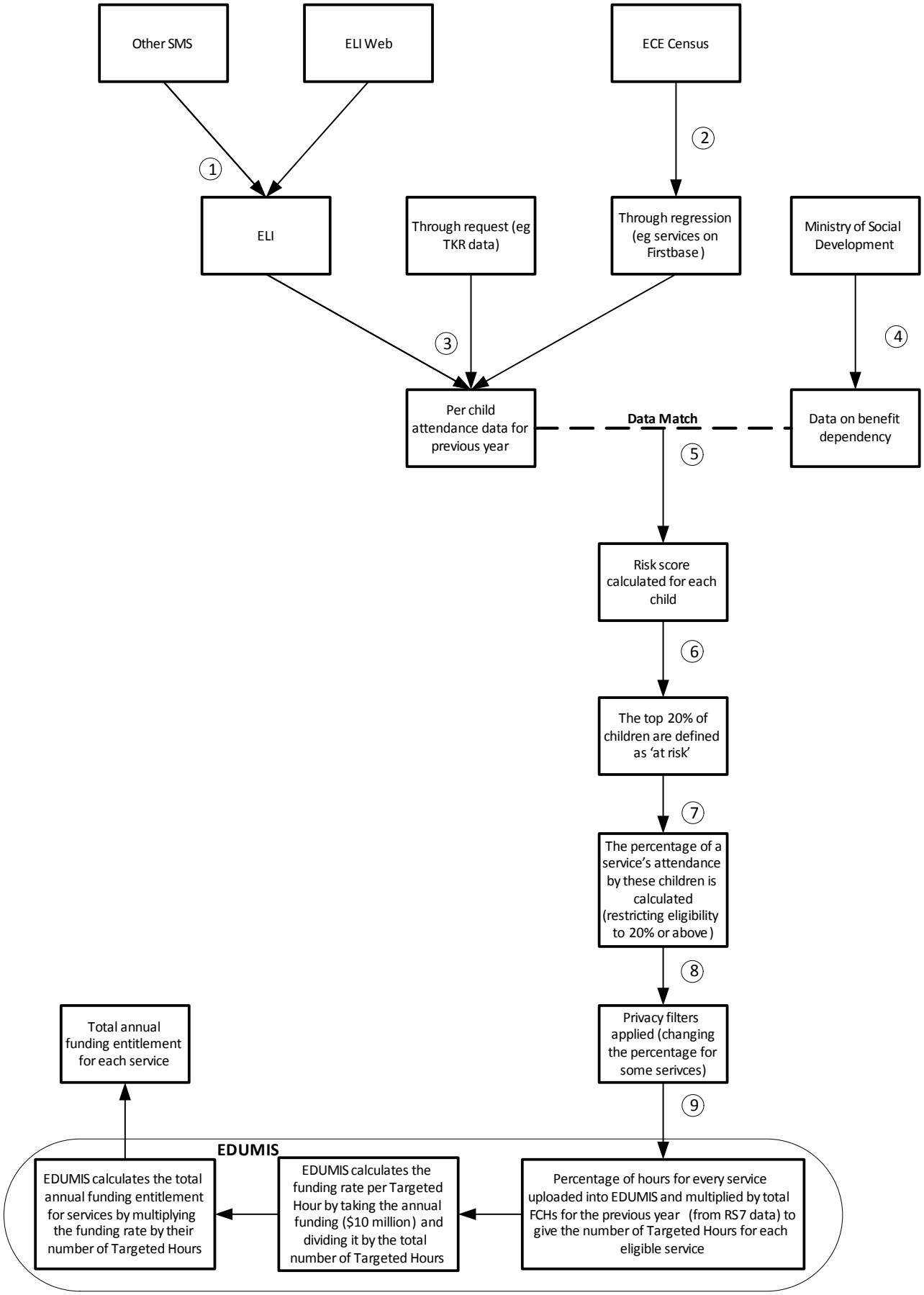
SYSTEM INTEGRATION

2.4.2 TFD integrates with other systems. The table below shows the direction of the dataflow.

System/service provider	Description	Internal	External	Data In	Data Out
MSD	Data on benefit receipt records will be received by MOE and matched with our per-child attendance data.		X	X	
ELI, run by MOE	Per-child attendance data will be extracted from ELI and matched with MSD data on benefit receipt.	X		X	
EDUMIS, run by MOE	The percentage of Targeted Hours for each service (with more than 20% of their FCH classified as Targeted Hours) will be uploaded to EDUMIS, which calculates the total annual funding entitlement for each service. At no point does EDUMIS contain any personal information.	X		X	X

2.4.3 The diagram below represents the information flows for the core processes of TFD. The table that follows details the personal information that is present in each of the numbered information flows.

Targeted Funding for Disadvantage Data Flow



Flow	Process/Activity	Description	Relevant Information
1.	Services submit their per-child attendance data to ELI using their SMS, either ELIWeb or a privately owned SMS.	This process is already occurring as services are obligated to submit data.	It is assumed that all the relevant risks here are captured under the ELI PIA.
2.	The relevant information is collected from the ECE Census data in order to perform a regression for services who are not submitting sufficient data to ELI (including Playcentre).	The regression compares ECE Census data for services without ELI data to those with sufficient ELI data.	The regression has already been run for modelling purposes.
3.	Per-child attendance data is collected from these three sources (ELI, TKR and the regression).	The data will be for the same one year period of 1 July – 30 June for all three sources.	The data from TKR is an updated version of the data they supplied the Ministry with for Funding Review modelling.
4.	As per a MOU, MSD provides MOE with two datasets, one on child level information and one on benefit period information.	The two datasets are linked by a parent ID (so the Ministry will not know the parent's identity).	Quality checks will be performed on this data by the Ministry. Whether a child is the dependent of a beneficiary or not will be known by the Ministry – new personal information.
5.	Per-child attendance data are matched with benefit receipt data to calculate a risk score for each child attending ECE.	The matching is done using the names and date of births of children.	Criteria have been determined for what can be matched (ie partial names).
6.	The 20% of children on the index are classed as 'at risk'.	The 20% are the children that have spent the highest proportion of their life as the dependent of a beneficiary.	New personal information will be created during this step (a risk score for children and whether they fall into the 20% category or not).
7.	The percentage of a service's attendance that is from children at risk of underachievement due to disadvantage is calculated.	The number of hours attended by children at risk of underachievement due to disadvantage is divided by the total hours of attendance for the service.	If the percentage is below 20% then a service will not receive any funding (and will not be entered into EDUMIS).
8.	The privacy filters are for particularly small services and services with high percentages.	Privacy filters will likely include rounding services with a percentage of Targeted Hours between 90% and 100% to 95% and excluding all services that	This is similar to the confidentiality thresholds that would be applied to the predictive risk index's use in the IDI, which uses rounding

Flow	Process/Activity	Description	Relevant Information
		have 4 or fewer children. This decision will be made in conjunction with Statistics NZ before the funding calculation is run.	to ensure individual children are not identified.
9.	The percentage of Targeted Hours is loaded into EDUMIS, which then gives the total annual funding entitlement for each eligible service.	The percentage of Targeted Hours multiplied by FCH from the previous year (from RS7 data) to estimate the number of Targeted Hours. This is then multiplied by the funding rate ($10million divided by the total number of Targeted Hours) to calculate services' annual funding entitlement.	No personal information is left at this stage. The funding rate will only be calculated in the first year. It will remain fixed in subsequent years.

3 Privacy analysis

The privacy analysis follows the information 'life cycle' of personal information, through its use, retention, processing, disclosure and destruction. It highlights how TFD changes any previous information handling practice and how this may affect individuals. This section of the report follows the IPPs and each paragraph includes:

- A reference back to the proposal with details how the proposal satisfies that IPP.
- Advantages of the proposal and any best practice that will be followed.
- A list of all privacy risks, (note that risk assessment will be completed in section 4, so risks are simply noted in this section.)

3.1 Principle 1 - purpose of collection of personal information

Principle 1 requires that the Ministry carefully considers the purpose for which it collects personal information. Having a clearly defined purpose will make it much easier to respond to obligations under the other Principles of the Act. The collection must be for a lawful purpose connected with a function or activity of the Ministry and collection must also be necessary for that purpose.

PURPOSE DETAIL

3.1.1 TFD will use existing data from ELI, MSD, TKR and the ECE Census to target additional funding to ECE services and ngā kōhanga reo with relatively high proportions of FCH attended by children at greater risk of educational underachievement due to disadvantage. The purpose of TFD is to:

- Use improvements in data analysis to more accurately target funding to ECE services and ngā kōhanga reo.
- Improve ECE affordability and quality for children from disadvantaged backgrounds and their families.
- Provide feedback for the Education Funding System Review, which will also use an index to identify children and young people at greater risk of educational underachievement due to disadvantage.
- All of these purposes are in line with functions or activities of the Ministry and therefore comply with Principle 1.

3.1.2 TFD will not require the collection of any new information. However, it will be using existing information for a different purpose:

- The information from MSD will be used to identify the proportion of each child's life they have been the dependent of a beneficiary.
- The information from ELI, TKR, and the ECE Census will be used to identify which services the children at risk of underachievement due to disadvantage attend and what percentage of a service's FCH are Targeted Hours.
- All of the information will be used to identify which children are at risk of educational underachievement due to disadvantage.
- This creates two new forms of personal information – whether a child is at risk or not and their risk score. The Ministry is creating this information rather than collecting it. However, if it was seen as collection, it would still be in line with the principle as it is for a lawful purpose and is connected with a function of the Ministry (funding ECE services).

PRIVACY RISKS

3.1.3 That unnecessary additional information is supplied; leading to the Ministry collecting and holding information it does not have a clear purpose for.

3.2 Principle 2 - source of personal information

Principle 2 is a statement of best practice, that personal information should be collected directly from the subject of the information. The best source of information about a person is usually the person him or herself. Also, collecting information from the person concerned means that people know what is going on and have some control over their information, but there are circumstances where it is impossible or not appropriate to collect the personal information from the person in question. There are also acceptable exceptions for this principle, such as when information is publically available, or the individual has authorised collection of information from someone else.

SOURCE DETAIL

3.2.1 Personal information is being collected from four different sources, none of which are the individual concerned. The four sources are listed below:

- MSD – the information being collected from MSD is benefit receipt records.
- ELI – the information being collected from ELI is per-child attendance data. ELI collects this information from services, who submit the data to the system via a SMS.
- ECE Census – the information being collected is per-child attendance data. This information is submitted by services, either through ELI or on an RS61 form.
- TKR – the information being collected is per-child attendance data. This information is collected by TKR from services.

3.2.2 The exceptions to the Principle the Ministry are adopting (which would apply to all sources of information):

- (2)(c) – that non-compliance would not prejudice the interests of the individual concerned.
- (2)(f) – that compliance is not reasonably practicable in the circumstances of the particular case.
- (2)(g)(ii) – that the information will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

PRIVACY RISKS

3.2.3 There are no privacy risks for TFD relating to this privacy principle.

3.3 Principle 3 - collection of information from subject

Principle 3 requires transparency between the collector of personal information and the subject as to why the information is being collected, who will hold it and who will have access to it. This Principle requires the Ministry and schools to do what is reasonable in the circumstances to make individuals aware of what their personal information will be used for and who may need access.

COLLECTION DETAIL

3.3.1 This Principle details the requirements for when the Ministry collects information directly from the individual concerned. This is not the case here as the Ministry is collecting the information from sources other than the individual concerned (see above at 4.2.1). The assumption is that the

relevant agencies will have collected the information in accordance with the Privacy Act. Therefore this Principle does not apply here.

PRIVACY RISKS

3.3.2 There are no privacy risks for TFD relating to this privacy principle.

3.4 Principle 4 - manner of collection of personal information

Principle 4 forbids the collection of personal information in ways that are unlawful, unfair, or that intrude to an unreasonable degree into the personal affairs of the individual, this Principle governs how information is collected.

MANNER DETAIL

3.4.1 TFD is not introducing new collection methods for information other than the collection of per-child attendance data from TKR. That was clearly framed as optional. TKR did not have to supply their data and it was made clear to them what the data would be used for if they did.

3.4.2 As mentioned in the assumptions, it is assumed that MSD collected their information in accordance with the Privacy Act and therefore this collection was lawful, fair and reasonable.

3.4.3 The information collected by ELI is covered by the ELI PIA and therefore it is assumed that the collection was in accordance with the Privacy Act and was lawful, fair and reasonable.

3.4.4 The information collected as part of the ECE Census is done lawfully, fairly and does not intrude to an unreasonable extent upon the personal affairs of the individuals concerned. It does not collect the names of children (although in some cases the reporting of children by gender, ethnicity and age could lead to particular children being identifiable). The service does not have to ask children or their families any additional information.

PRIVACY RISKS

3.4.5 There are no privacy risks for TFD relating to this privacy principle.

3.5 Principle 5 - storage and security of personal information

Principle 5 requires the Ministry to ensure that the personal information it holds, is protected by adequate security safeguards against loss, misuse or unauthorised access.

STORAGE & SECURITY DETAIL

3.5.1 At the time of this report, TFD has not been subject to an information security risk assessment.

3.5.2 The Ministry is subject to the guidelines issued by the Government Chief Information Officer that require appropriate information risk management, security and assurance.

3.5.3 The Ministry asserts that well-established policies, procedures, and systems are in place to ensure adequate measures of physical and electronic security.

3.5.4 The information held for the funding calculation will be stored on a secure drive, only accessible from the Ministry's network, which is not internet facing. Only those authorised to access the information, approximately five users, will be able to view the folder within the secure drive.

3.5.5 All of the TFD processes will be internal to the Ministry, including the funding calculation, which will take place in EDUMIS.

3.5.6 The information from MSD and TKR will only be held by the Ministry for approximately two months per year (to allow time for quality checks, the funding calculation, and quality assurance) and then deleted, minimising the risk of a privacy breach.

3.5.7 Personal information about whether a child is 'at risk' or not and their risk score will be held for less than a week before it is securely deleted (to allow time for quality assurance).

3.5.8 ELI information and ECE Census information is already permanently held by the Ministry.

3.5.9 Information supplied by MSD and TKR will be securely transported via Ironkey.

PRIVACY RISKS

3.5.10 That someone within the Ministry who is not authorised to access the information does so.

3.5.11 That an unauthorised person gains access to personal information as it is in transit, leading to unauthorised disclosure.

3.5.12 That a Ministry employee accidentally discloses, modifies or removes personal information they are not authorised to.

3.5.13 That a Ministry employee deliberately discloses, modifies or removes personal information they are not authorised to.

3.5.14 That security controls within the Ministry are insufficient, leading to a malicious attack from an external source that carries out unauthorised disclosure of personal information.

3.6 Principle 6 - access to personal information

Principle 6 requires that individuals have the right to access personal information that the Ministry holds about them.

ACCESS DETAIL

3.6.1 Any requests for access of MSD benefit receipt data or TKR per-child attendance data will be transferred to MSD or TKR under s 39(b)(ii) of the Privacy Act 1993. That states that "where the information to which the request relates is believed by the person dealing with the request to be more closely connected with the functions or activities of another agency, the agency to which the request is made shall promptly, and in any case not later than 10 working days after the day on which the request is received, transfer the request to the other agency and inform the individual making the request accordingly."

3.6.2 This is because the information that the Ministry temporarily holds on benefit receipt or per-child attendance will be a duplicate of the information that MSD or TKR permanently holds. Information on benefit receipt is clearly more closely connected with the functions and activities of MSD. Information on the attendance of children in TKR services is more closely connected with the functions and activities of TKR.

3.6.3 In addition, the information that the Ministry holds on benefit receipt will not include the names of benefit recipients, only their children. This means that much of the information (eg period of time on benefit, type of benefit) could not be accessed or corrected.

3.6.4 The ELI data can be requested through the Ministry already, as outlined in the ELI PIA from 2014, which states "children's personal details, and the NSN record can be accessed by the parent or guardian concerned through the Ministry of Education."

3.6.5 The ECE Census data can also be requested through the Ministry already. There is a link on the Ministry website to a specific email for individuals wishing to access or correct their personal information (privacy@education.govt.nz) and a physical address, which will be available to individuals wishing to access their ELI or ECE Census data.

3.6.6 The Ministry will also be creating two new forms of personal information – whether a child will be classed as 'at risk' for that year's funding calculation and their risk score. This information will only in be held in a personally identifiable form by the Ministry for approximately a week every year while the data match is quality assured. Requests for this information by a parent of a child will be declined

under s 29(1)(a) of the Privacy Act as it could reveal personal information about the other parent – whether they have been on a benefit or not.

3.6.7 In addition to this, for most of the year, when the Ministry does not hold the information on which children are classed as 'at risk', requests for information will also be refused under s 29(2)(b) as the information does not exist.

PRIVACY RISKS

3.6.8 That requests for access or correction of personal information are unlawfully denied.

3.6.9 That requests for access or correction of personal information are not transferred to the relevant agency in a timely manner under s 39 of the Privacy Act 1993.

3.7 Principle 7 - correction of personal information

Principle 7 requires that individuals have the right to request the correction of personal information.

CORRECTION DETAIL

3.7.1 As with the access to personal information, requests for correction of MSD or TKR data will be transferred to MSD or TKR under s 39(b)(ii) of the Privacy Act 1993. The justification for this is the same as the justification for why we will be transferring requests for access to personal information (see above at 4.6.1).

3.7.2 In addition to this, correction of the benefit receipt data or per-child attendance data that MOE held would not have any impact as the information will be deleted after the funding calculation is complete each year.

3.7.3 Requests for correction of personal information relating to ELI or ECE Census data will be managed through the existing process, where individuals are able to email or post a request to the Ministry.

3.7.4 As requests to access personal information about a child's risk score and classification will be declined, this information will not be able to be corrected.

PRIVACY RISKS

3.7.5 That requests for access or correction of personal information are unlawfully denied.

3.7.6 That requests for access or correction of personal information are not transferred to the relevant agency in a timely manner under s 39 of the Privacy Act 1993.

3.8 Principle 8 - accuracy of personal information to be checked before use

Principle 8 requires the Ministry to take all reasonable steps to ensure the accuracy of personal information before it is used and on an ongoing basis.

ACCURACY DETAIL

3.8.1 ELI Data Extraction Business Rules have been formulated to ensure the ELI data used in the funding calculation is accurate, up-to-date, complete, relevant, and not misleading. This includes rules such as what is excluded to ensure data quality and the minimum length of attendance data that is needed.

3.8.2 In addition there are a series of data quality procedures that have already been put in place as part of the ELI PIA. This includes field validation upon entry of data, record level validation of data prior to submission to the Ministry, validation through a rules based validation tool (managed by data quality staff), further validation through various reports, and manual validation where necessary.

3.8.3 Information from MSD will undergo data quality assurance by looking at the linkage between the two tables received, the number of children and matching parents, the period covered, duplicate records and type of benefits.

3.8.4 Information from TKR will undergo a similar data quality check to MSD information, and both will have any irrelevant information in the data sets deleted.

PRIVACY RISKS

3.8.5 That a match does not occur where it should, or occurs where it should not, due to a lack of consistency between names in different datasets or record systems.

3.9 Principle 9 – agency not to keep personal information for longer than necessary

Principle 9 requires the Ministry to keep that information for no longer than is required for the purposes for which the information may lawfully be used.

RETENTION DETAIL

3.9.1 The Ministry will securely delete the personal information it holds once the percentage of Targeted Hours has been determined.

3.9.2 There will be no obligation under law for the Ministry to keep that information any longer. This is because the information will still be held in the original sources that it came from – ie ELI, MSD, or the ECE Census data.

PRIVACY RISKS

3.9.3 That personal information is not securely deleted after it is no longer required for the stated purpose, leading to ongoing security risks and the potential for it to be used in ways that were not envisioned, such as another project.

3.10 Principle 10 - limits on use of personal information

Principle 10 requires that the Ministry does not use personal information for any other purpose than that which it was originally obtained for.

LIMITED USE DETAIL

3.10.1 The Ministry will be using personal information for a different purpose than that for which it was originally obtained for; it will be using it to calculate funding.

3.10.2 The Ministry is able to do this and still comply with Principle 10 because it falls under one of the exceptions listed in the Privacy Act. That is that the Ministry believes, on reasonable grounds, that the information is used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

3.10.3 This exception applies as the children will not be named and privacy filters will be put in place to ensure that children cannot be identified from a service's percentage of Targeted Hours. These will be decided in conjunctions with Statistics New Zealand before the funding calculation is run.

PRIVACY RISKS

3.10.4 That the percentage of Targeted Hours a service receives enables them to identify which children are classified as 'at risk'.

3.10.5 That the Ministry decides to use personal information for a different use that does not fall within the statistical purposes exception.

3.11 Principle 11 - limits on disclosure of personal information

Principle 11 prohibits the Ministry from disclosing personal information unless directly related to the purpose it was collected for.

LIMITED DISCLOSURE DETAIL

3.11.1 The organisations that are providing personal information to the Ministry (MSD and TKR) are entitled to expect information sharing within the organisation is limited and takes place only in relation to the purpose for which the information as collected from them.

3.11.2 There is no reason why the Ministry would disclose personal information to any person or body or agency. The information being given to services will be strictly at a service level and the children identified as 'at risk' will not be identified.

PRIVACY RISKS

3.11.3 That an unauthorised person gains access to personal information as it is in transit.

3.11.4 That a Ministry employee accidentally discloses, modifies or removes personal information they are not authorised to.

3.11.5 That a Ministry employee deliberately discloses, modifies or removes personal information they are not authorised to.

3.11.6 That security controls within the Ministry are insufficient, leading to a malicious attack from an external source that carries out unauthorised disclosure of personal information.

3.11.7 That the percentage of Targeted Hours a service receives enables them to identify which children are classified as 'at risk'.

3.11.8 That personal information is shared with one of the agencies that have provided some of the information used.

3.12 Principle 12 - unique identifiers

Principle 12 seeks to restrict the assignment of unique identifiers to individuals.

UNIQUE IDENTIFIER DETAIL

3.12.1 TFD will not assign any new unique identifiers.

3.12.2 Children within ELI are currently assigned a unique identifier, their National Student Number (NSN). This information will not be extracted from ELI, as NSNs are not being used in the matching with MSD benefit receipt data, instead names and dates of births are being used instead.

PRIVACY RISKS

3.12.3 There are no privacy risks for TFD relating to this privacy principle.

4 Privacy risk assessment

4.1 Privacy Risk Assessment

The risks highlighted in the Privacy Analysis are collated and assessed in the table below. Privacy enhancing response numbers (e.g. PR1, PR2) refer to the privacy enhancing responses in section 6.1. Control numbers (e.g. C1, C2) refer to the controls in section 5.2. Further explanations of the privacy enhancing responses and controls are given there.

Risk ID	Affected Privacy Principle(s)	Risk Description	Risk Scenario(s)	Key Risk Drivers	Inherent Risk			Privacy Enhancing Responses and Controls (explained in greater depth in section 6.1 and section 6.2)	Residual Risk			Explanation
					Likelihood	Impact	Risk Rating		Likelihood	Impact	Risk Rating	
R1.	Principle 1	That unnecessary additional information is supplied; leading to the Ministry collecting and holding information it does not have a clear purpose for.	TKR or MSD supply the Ministry with not only the information requested but also unnecessary additional information.	• TKR have previously supplied us with per-child attendance information for modelling purposes and supplied extra information. This could happen again. • The required data specifications are not clearly defined and agreed.	LIKELY	MINOR	LOW	• PR1 – MSD filters. • C1 – Memorandum of Understanding or Agreement. • C2 – Media Sanitisation and Disposal.	POSSIBLE	MINOR	LOW	MSD will apply filters to the benefit receipt records supplied so only those records with children in the correct age range are supplied, detailed in the Memorandum. Data specifications are clearly defined in an MOU or Agreement with MSD or TKR, detailing the exact information required. Any additional information supplied to the Ministry that was not needed will be securely deleted immediately.
R2.	Principle 5	That someone within the Ministry who is not authorised to access the information does so.	Information is not kept in a secure file and an unauthorised employee is able to access the information. An unauthorised employee who was previously authorised may retain their access.	• Access permission required for the roles may not be configured properly. • Staff members who are no longer authorised may not have their access removed. • A staff member may circumvent a process. • The EDK restructure may lead to confusion around people's roles.	UNLIKELY	MEDIUM	LOW	• PR2 – The Ministry Privacy Policy and Awareness. • C3 – Code of Conduct. • C4 – Contractual Agreements. • C5 – Management of Privileged Access. • C9 – Move, Add, Change and Delete.	RARE	MEDIUM	LOW	Management of privileged access will mean that only authorised employees will have access to personal information. Non-disclosure agreements will be signed by all employees (permanent/temporarily contracted) who are authorised to access personal information.

Risk ID	Affected Privacy Principle(s)	Risk Description	Risk Scenario(s)	Key Risk Drivers	Inherent Risk			Privacy Enhancing Responses and Controls (explained in greater depth in section 6.1 and section 6.2)	Residual Risk			Explanation
					Likelihood	Impact	Risk Rating		Likelihood	Impact	Risk Rating	
R3.	Principles 5, 11	That an unauthorised person gains access to personal information as it is in transit, leading to unauthorised disclosure.	An agency emails information to the wrong email address. An agency gives the Ministry their information on an unencrypted USB which is dropped in transit and then picked up by someone else.	• Sending information in the same manner as it has been done in the past. • Inadequate training and education of privacy policy. • Lack of clarity in an MOU around how personal information should be transferred between parties supplying data and the Ministry.	UNLIKELY	SUBSTANTIAL	HIGH	• PR2 – The Ministry Privacy Policy and Awareness. • PR3 – Privacy Incident Management Process. • PR4 – Media Engagement Strategy. • C1 – Memorandum of Understanding or Agreement. • C6 – People and Capability Processes. • C7 – Encryption of Data in Transit.	RARE	MAJOR	MODERATE	Agencies supplying information to the Ministry will be clearly advised of how information will be transferred between the Ministry and agency. An ironkey will be used to transfer information with the password either emailed or phoned through separately.
R4.	Principles 5, 11	That a Ministry employee accidentally discloses, modifies or removes personal information they are not authorised to.	A Ministry employee accidentally deletes personal information before it has been used. An authorised employee shares personal information with an unauthorised employee believing they are authorised to view this information. A Ministry employee shares personal information to an unauthorised external person, not realising that it is unauthorised disclosure.	• Inadequate training and education of privacy policy. • Access permission required for the roles may not be configured properly. • Staff members who are no longer authorised may not have their access removed. • The EDK restructure may lead to confusion around people's roles.	UNLIKELY	SUBSTANTIAL	HIGH	• PR2 – The Ministry Privacy Policy and Awareness. • PR3 – Privacy Incident Management Process. • PR4 – Media Engagement Strategy. • C3 – Code of Conduct. • C4 – Contractual Agreements. • C5 – Management of Privileged Access. • C6 – People and Capability Processes. • C8 – Logging and Auditing.	RARE	MAJOR	MODERATE	There will only be a very limited time period where this risk could occur, before the personal information is deleted. Ensure all temporary and permanent Ministry employees are aware of their obligations around keeping personal information secure.
R5.	Principles 5, 11	That a Ministry employee deliberately discloses, modifies or removes personal information they are not authorised to.	A Ministry employee leaks information to the media around which children are at risk. A Ministry employee discloses to a friend that their child is classified as 'at risk'. A Ministry employee discloses to a friend with an ECE service which children attending are classified as 'at risk'.	• Absence of monitoring controls or database triggers that detect suspicious data accesses or moves. • Disgruntled staff members, including those upset by the EDK restructure. • A staff member may circumvent a process. • Political motivation.	RARE	SUBSTANTIAL	MODERATE	• PR3 – Privacy Incident Management Process. • PR4 – Media Engagement Strategy. • C3 – Code of Conduct. • C4 – Contractual Agreements. • C5 – Management of Privileged Access. • C6 – People and Capability Processes. • C8 – Logging and Auditing. • C9 – Move, Add, Change and Delete.	RARE	MAJOR	MODERATE	There will only be a very limited time period where this risk could occur, before the personal information is deleted.

Risk ID	Affected Privacy Principle(s)	Risk Description	Risk Scenario(s)	Key Risk Drivers	Inherent Risk			Privacy Enhancing Responses and Controls (explained in greater depth in section 6.1 and section 6.2)	Residual Risk			Explanation
					Likelihood	Impact	Risk Rating		Likelihood	Impact	Risk Rating	
R6.	Principles 5, 11	That security controls within the Ministry are insufficient, leading to a malicious attack from an external source that carries out unauthorised disclosure of personal information.	A targeted attack from a motivated external source.	• Security flaws. • Inadequate assurance of security. • A lack of explanation to the public around how funding is calculated and how the privacy of individuals is protected during the process.	RARE	SUBSTANTIAL	MODERATE	• PR3 – Privacy Incident Management Process. • PR4 – Media Engagement Strategy. • PR5 – Communication Strategy. • PR6 – Privacy Statement. • C10 – Information Security Reviews.	RARE	MAJOR	MODERATE	There will only be a very limited time period where this risk could occur, before the personal information is deleted. All of the information will be held on the Ministry's internal network.
R7.	Principles 6, 7	That requests for access or correction of personal information are unlawfully denied.	A Ministry employee dealing with a request does not realise we hold the information (ie the classification of whether a child is 'at risk' or not).	• Some of the personal information (the TKR information, the MSD information and the classification of children as 'at risk') is only held by the Ministry for a short period every year. • A new form of personal information is being held.	UNLIKELY	MINOR	VERY LOW	• PR2 – The Ministry Privacy Policy and Awareness. • C6 – People and Capability Processes. • C11 – Information Correction Process.	RARE	MINOR	VERY LOW	There will only be a very limited time period where this risk could occur, before the personal information is deleted, in particular the information on whether children are 'at risk' will be held for a week. It is unlikely (especially in the first year) that anyone will request this information during that period.
R8.	Principles 6, 7	That requests for access or correction of personal information are not transferred to the relevant agency in a timely manner under s 39 of the Privacy Act.	A Ministry employee dealing with a request does not realise that it is to be transferred to MSD or TKR under s 39 of the Privacy Act 1993 and must be transferred within 10 working days. A request may be sent to the wrong email address within the Ministry and not reach the correct person in time for the request to be transferred within 10 working days.	• The personal information from TKR and MSD is only held by the Ministry for a short period every year. • The Ministry may receive a large number of requests in a short period of time, especially in subsequent years as people become more aware of the timing of the process and what information the Ministry holds.	POSSIBLE	MINOR	LOW	• PR2 – The Ministry Privacy Policy and Awareness. • PR7 – Online Link. • C1 – Memorandum of Understanding or Agreement. • C6 – People and Capability Processes. • C11 – Information Correction Process. • C16 – Retention Requirements.	UNLIKELY	MINOR	VERY LOW	There will only be a very limited time period where this risk could occur, before the personal information is deleted. The website page on TFD will be updated to include a general help email, to help ensure emails reach the right destination.

Risk ID	Affected Privacy Principle(s)	Risk Description	Risk Scenario(s)	Key Risk Drivers	Inherent Risk			Privacy Enhancing Responses and Controls (explained in greater depth in section 6.1 and section 6.2)	Residual Risk			Explanation
					Likelihood	Impact	Risk Rating		Likelihood	Impact	Risk Rating	
R9.	Principle 8	That a match does not occur where it should, or occurs where it should not, due to a lack of consistency between names in different datasets or record systems.	The correct full name of a child recorded by MSD in their benefit receipt records is not the same as the preferred name that is recorded by a service when entering a child into ELI so a match between the two records is not made.	• The Ministry only suggests that a service should check a child's details with their official identification documentation when creating a record of them within ELI, it is not compulsory. • MSD benefit receipt records can contain a range of different names and aliases for different individuals.	UNLIKELY	MINOR	VERY LOW	• PR3 – Privacy Incident Management Process. • PR5 – Communication Strategy. • C1 – Memorandum of Understanding or Agreement. • C12 – Data Cleansing.	RARE	MINOR	VERY LOW	Services will be made aware that they need to ensure a child's correct full name is uploaded to ELI. The use of dates of births in the matching procedure will help to mitigate any discrepancies in names.
R10.	Principle 9	That personal information is not securely deleted after it is no longer required for the stated purpose, leading to ongoing security risks and the potential for it to be used in ways that were not envisioned, such as another project.	Information is not fully deleted from the Ministry's systems. Information is kept because it could be useful later on.	• Inadequate training and education of privacy policy. • The personal information could be seen as useful for another project. • A lack of clear instruction about when and how information should be deleted. • The EDK restructure may lead to confusion around people's roles. • A delay in the funding calculation could mean the information is kept for longer than planned.	LIKELY	MINOR	LOW	• PR2 – The Ministry's Privacy Policy and Awareness. • C2 – Media Sanitisation and Disposal. • C3 – Code of Conduct. • C4 – Contractual Agreements. • C5 – Management of Privileged Access. • C6 – People and Capability Processes. • C9 – Move, Add, Change and Delete. • C10 – Information Security Reviews. • C14 – Encryption at Rest. • C15 – Information Classification. • C16 – Retention Requirements.	UNLIKELY	MINOR	VERY LOW	A date range will be given for the deletion to account for any delays in the funding calculation.
R11.	Principles 10, 11	That the percentage of Targeted Hours a service receives enables them to identify which children are classified as at risk.	A service may have a small number of children attending, which may allow for an inference to be made as to those considered 'at risk'. The calculation may result in 100% of a service's hours being classified as Targeted Hours, allowing them to identify all the children that were attending during the data collection period as 'at risk'.	• Modelling has shown that some services will likely have 100% of their hours classified as Targeted Hours. • Services with small numbers of children may know which children are more likely to meet the criteria for being classified as 'at risk'.	ALMOST CERTAIN	MEDIUM	HIGH	• PR3 – Privacy Incident Management Process. • PR4 – Media Engagement Strategy. • PR5 – Communication Strategy. • PR8 – Confidentiality Thresholds.	RARE	MEDIUM	LOW	Services with 4 or fewer children will be excluded from the funding calculation. The percentage will likely be rounded to 95% for services with a percentage between 90% and 100% (and to 80% for services with fewer than 10 children and a percentage between 80% and 100%.)

Risk ID	Affected Privacy Principle(s)	Risk Description	Risk Scenario(s)	Key Risk Drivers	Inherent Risk			Privacy Enhancing Responses and Controls (explained in greater depth in section 6.1 and section 6.2)	Residual Risk			Explanation
					Likelihood	Impact	Risk Rating		Likelihood	Impact	Risk Rating	
R12.	Principle 10	That the Ministry decides to use the information for a different use that does not fall within the statistical purposes exception.	A situation arises where the personal information could be useful in another context within the Ministry but it is not for statistical or research purposes or requires the information to be published in an identifiable form.	• Inadequate training and education of privacy policy. • A lack of clear understanding on how the personal information can only be used as long as it complies with Principle 10, including the exceptions.	UNLIKELY	MEDIUM	LOW	• PR2 – The Ministry Privacy Policy and Awareness. • C2 – Media Sanitisation and Disposal. • C3 – Code of Conduct. • C4 – Contractual Agreements. • C5 – Management of Privileged Access. • C6 – People and Capability Processes. • C9 – Move, Add, Change and Delete.	RARE	MINOR	VERY LOW	The purpose of the data will be made clear to everyone involved. The deletion of the data will reduce the chance that this risk occurs. A limited number of Ministry employees being able to access the data will also limit the chance of the risk occurring.
R13.	Principle 11	That personal information is shared with one of the agencies that have provided some of the information used.	MSD requests that we provide them with a list of children who are not attending ECE and are also currently part of a benefit dependent household. TKR requests a list of the children attending their services who are currently the dependent of a beneficiary.	• A lack of clear understanding about what each agency will and will not receive. • Inadequate training and education of privacy policy.	UNLIKELY	MEDIUM	LOW	• PR2 – The Ministry Privacy Policy and Awareness. • PR3 – Privacy Incident Management Process. • PR4 – Media Engagement Strategy. • C1 – Memorandum of Understanding or Agreement. • C3 – Code of Conduct. • C4 – Contractual Agreements. • C5 – Management of Privileged Access. • C6 – People and Capability Processes. • C13 – Identification of Applicable Legislation.	RARE	MINOR	VERY LOW	A limited number of Ministry employees being able to access the data will limit the chance of the risk occurring as there will be fewer people to provide information where they should not. The Memorandum and Agreement will clarify for other agencies what the data can be used for and that we cannot provide any information in return.

5 Privacy Enhancing Responses and Controls

This section describes the recommended actions to treat privacy risks and/or enhance the privacy of personal information for TFD.

5.1 Privacy Enhancing Responses

5.1.1 The following are the recommended privacy enhancing responses, designed to enhance the privacy of personal information collected for TFD.

ID	Privacy Enhancing Response	Description	Risk Mapping
PR1	MSD filters.	MSD will put in place filters to ensure that only benefit receipt records relating to children in the correct age range are supplied.	1
PR2	The Ministry Privacy Policy and Awareness.	Reiterate the Ministry Privacy Policy for Ministry employees who will be dealing with personal information.	2, 3, 4, 8, 10, 12, 13
PR3	Privacy Incident Management Process.	Ensure the Ministry has an established Privacy Breach Investigation Process that follows the Office of the Privacy Commissioner recommendation for privacy breaches.	3, 4, 5, 6, 9, 11, 13
PR4	Media Engagement Strategy.	Develop a media engagement strategy to communicate the Ministry messages in the event of an actual or suspected privacy incident or breach.	3, 4, 5, 6, 11, 13
PR5	Communication Strategy.	Ensure that the public is aware of the fact that no personal information will be released and services will only receive a percentage of Targeted Hours.	6, 9, 11
PR6	Privacy Statement.	Ensure a Privacy Statement specifically for TFD is produced.	6
PR7	Online Link.	Place a link to an email address on the website with other information on TFD to ensure privacy requests are seen in a timely manner.	7, 8
PR8	Confidentiality Thresholds.	Put in place privacy filters that are sufficient to protect the privacy of children. These will be decided in conjunction with Statistics New Zealand before the funding calculation is run.	11

5.2 Controls

5.2.1 Following are the recommended controls (in addition to the privacy responses above) that are based on the privacy risks identified in section 4. These controls will facilitate the reduction in inherent risk to the levels of residual risk indicated.

ID	Control	Description	Risk Mapping
C1.	Memorandum of Understanding or Agreement.	The Ministry should take steps to ensure they have an up-to-date Memorandum of Understanding with MSD that reflects the	1, 3, 8, 9, 13

ID	Control	Description	Risk Mapping
		privacy risks in this document. They should also ensure the same is done in an agreement with TKR.	
C2.	Media Sanitisation and Disposal.	Ensure that all information that is no longer needed is securely deleted.	1, 10, 12
C3.	Code of Conduct.	All Ministry employees must have read and signed the Code of Conduct.	2, 4, 5, 10, 12, 13
C4.	Contractual Agreements.	Any contractors that are granted access to personal information must sign a non-disclosure agreement.	2, 4, 5, 10, 12, 13
C5.	Management of Privileged Access.	The allocation, maintenance and removal of privileged access rights will be controlled through formal authorisation processes.	2, 4, 5, 10, 12, 13
C6.	People and Capability Processes.	The Ministry should ensure it has appropriate human resources processes in place and that they are followed, including induction for new staff covering information security, changes in employee circumstances and behaviour are monitored and managed and formal disciplinary procedures for staff that breach information security policies are in place. It should also ensure that skill shortages or dependence on individual staff members are managed and minimised.	3, 4, 5, 7, 8, 10, 12, 13
C7.	Encryption of Data in Transit.	Any data that is sent to the Ministry is appropriately encrypted.	3
C8.	Logging and Auditing.	Monitoring controls are in place, which detect suspicious data accesses or moves.	4, 5
C9.	Move, Add, Change and Delete.	The unique user's allocated specific roles within the solution must follow a formal access control process, including requests for access, approval, granting and removal of access, as well as a regular revalidation process.	2, 5, 10, 12
C10.	Information Security Reviews.	The security of personal information is regularly reviewed.	6, 10
C11.	Information Correction Process.	There is an information correction process in place that allows individuals to request correction of their personal information.	7, 8
C12.	Data Cleansing.	Data is checked for inconsistencies and quality issues.	9
C13.	Identification of Applicable Legislation.	Legislation that could override the Privacy Act and allow the Ministry to disclose personal information is identified.	13
C14.	Encryption at Rest.	Ensuring business sensitive, private, or otherwise classified information stored on media is encrypted using approved encryption	10

ID	Control	Description	Risk Mapping
		algorithms and protocols, reduces the likelihood of unauthorised disclosure.	
C15.	Information Classification.	Information shall be classified in terms of legal requirements, value, criticality, and sensitivity to unauthorised disclosure or modification. Official information shall be classified using the New Zealand Government Classification System.	10
C16.	Retention Requirements.	Develop, determine and observe the appropriate retention requirements for personal information processed on system.	8, 10

6 Compliance mechanisms

6.1.1 Following are recommendations to ensure that TFD remains compliant with the Privacy Act therefore ensuring the privacy of the personal information collected in the future.

- Many of the privacy enhancing responses and controls identified in this report will assist in assuring ongoing compliance with the Privacy Act if they are adhered to, so it is recommended they are implemented.
- The Ministry should revisit the PIA each time a major change is proposed to TFD to ensure that any new risks are captured and addressed.